## *REMARKS*

This is a full and timely response to the outstanding Office Action mailed July 24, 2006. Reconsideration and allowance of the application and presently pending claims are respectfully requested.

1. Response to Rejection of Claims Under 35 U.S.C. § 102(e)

Claims 1-11, 13-23, and 25-41 have been rejected under 35 U.S.C. § 102(e) as being anticipated by *Schwartz* (U.S. Patent Application Publication 2002/0199114 A1). Applicant respectfully traverses the rejections.

It is axiomatic that "[a]nticipation requires the disclosure in a single prior art reference of each element of the claim under consideration." *W. L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1554, 220 USPQ 303, 313 (Fed. Cir. 1983). Therefore, every claimed feature of the claimed invention must be represented in the applied reference to constitute a proper rejection under 35 U.S.C. § 102(e).

In the present case, not every feature of the claimed invention is represented in the *Schwartz* reference. Applicant discusses the *Schwartz* reference and Applicant's claims in the following.

a. Applicants' claims

In general, Applicants' claims are directed to at least one embodiment, among others, where a transmission device 100 attempts to transmit data to a destination that is protected by a firewall 20. The transmission device 100 searches for an address of the firewall 20 (that is protecting the destination) that will allow the data to pass to the destination.

b. *Schwartz* Reference

In general, *Schwartz* teaches embodiments where a transmission device is protected by a firewall and the transmission device attempts to locate an address of the firewall (that is protecting the transmission device) that will allow a connection to be established with the firewall 20 for outside communications.

Accordingly, *Schwartz* discusses how non-traditional devices generally do not have interfaces for configuring the devices for communications with a

local firewall. *See* para. 0024. *Schwartz* also discusses how it is necessary for information to be "transferred from the non-traditional devices across from the LAN 311 through the firewall 310 [which services the non-traditional devices] to a destination." *See* Figure 3 and para. 0025. *Schwartz* further discusses how devices often use DHCP to obtain a local IP address for communicating, but that the device may also be configured manually to communicate with the local firewall. Otherwise, an approach of trying different addresses may be used. *See* para. 0026. *Schwartz* also discusses that a connection with a local firewall must be established before communications with entities on the other side of the firewall are possible. *See* para. 0027. *Schwartz* further discusses that a device may sniff packets on a local network to attempt to determine an address and port of a firewall on the local network that allows external communications beyond the firewall. *See* para. 0034.

c. Claim 1

As provided in independent claim 1, Applicant claims:

> A method of transmitting data across a firewall, the method comprising:
> ***receiving a request to transmit data to a destination at a remote network;***
> ***searching for a firewall associated with the destination at the remote network***, the firewall being configured to prohibit communication to the destination via a primary communication protocol and allow communication to the destination via a secondary communication protocol;
> ***if the firewall is detected, automatically configuring the data for communication with the secondary communication protocol;*** and
> transmitting the data to the destination by utilizing the secondary communication protocol, ***wherein the request to transmit the data to the destination comprises a primary address of the destination related to the primary communication protocol and a secondary address of the destination related to the secondary communication protocol.***

(Emphasis added).

Applicant respectfully submits that independent claim 1 is allowable for at least the reason that *Schwartz* does not disclose, teach, or suggest at least

"receiving a request to transmit data to a destination at a remote network," "searching for a firewall associated with the destination at the remote network," "if the firewall is detected, automatically configuring the data for communication with the secondary communication protocol," and "wherein the request to transmit the data to the destination comprises a primary address of the destination related to the primary communication protocol and a secondary address of the destination related to the secondary communication protocol," as recited and emphasized above.

Rather, *Schwartz* discloses at most a system for configuring a device to communicate through a firewall on a local network, where the device is also located on the local network. *See* paras. 0024-0025. *See* Figure 3 (*e.g.*, devices 312, 314, and firewall 310). *Schwartz* fails to teach or suggest searching for a firewall associated with a destination at a remote network.

*Schwartz* also states that "if an address and/or port does not yield a successful connection, then the next time the device will select the most likely address and port 506, it may not include the unsuccessful port." *See* para. 0032. "It is to be understood that select most likely address and port 506 is based upon a database of addresses and ports and that this database changes." *See* para. 0032. Therefore, *Schwartz* fails to teach or suggest that a request to transmit data includes a primary address of the destination that is used if a firewall is not detected and a secondary address of the destination that is used if a firewall is detected, as described in the claim. Rather, *Schwartz* uses whatever port the non-traditional device discerns is most likely to establish a connection with the local firewall. As such, *Schwartz* fails to teach or suggest that a request to transmit data includes a primary address and a secondary address of a <u>firewall associated with a destination</u>. As previously indicated, *Schwartz* teaches that a local device is configured to operate with a local firewall by attempting different addresses for the local firewall. No where does it teach or suggest attempting to communicate with a firewall associated with a destination at a remote network in a manner described by the claim.

For at least these reasons, *Schwartz* fails to anticipate claim 1. In the Office Action, it states that "the client shown in Fig. 3 may have to pass the

firewall associated with the appliances in the remote network to control them." Page 3. However, no where in *Schwartz* does it state that the clients 308-1...308-N shown in Fig. 3 perform the method for firewall traversal disclosed in the reference. Rather, the non-traditional devices 314-1...314-Q are disclosed to employ the method for firewall traversal described in the reference which states "This information must be transferred from the non-traditional device across the LAN 311 through the firewall 310 to a destination." Para. 0025. Another example is provided in *Schwartz* of a home entertainments system 314-5 that must traverse the local firewall 310 to access the manufacturer's site. As such, *Schwartz* does not teach "searching for a firewall associated with the destination at the remote network . . . wherein the request to transmit the data to the destination comprises a primary address of the destination related to the primary communication protocol and a secondary address of the destination related to the secondary communication protocol," as recited in claim 1.

Moreover, the Office Action states that "It is true that Scharwtz won't try the primary address again if it fails, but it clearly tries it the first time, which was before the connection failed. Therefore, the address of the primary and secondary protocols must be received by the device that initiates the connection." Page 4. Applicants respectfully disagree, since *Schwartz* teaches that an address may be obtained by sniffing network traffic and therefore does not have to be "received by the device that initiates the connection." Further, *Schwartz* does not teach or suggest that a request to transmit data comprises both the primary address and secondary address of the destination, as described in claim 1.

For at least these reasons, *Schwartz* fails to anticipate claim 1, and the rejection of claim 1 should be withdrawn.

d. Claims 2 and 4-13

Because independent claim 1 is allowable over the cited art of record, dependent claims 2 and 4-13 (which depend from independent claim 1) are allowable as a matter of law for at least the reason that the dependent claims

2 and 4-13 contain all the steps and features of independent claim 1. For at least this reason, the rejection of claims 2 and 4-13 should be withdrawn.

Additionally and notwithstanding the foregoing reasons for allowability of claims 2 and 4-13, these claims recite further features and/or combinations of features (as is apparent by examination of the claims themselves) that are patentably distinct from the cited art of record. Hence, there are other reasons why these dependent claims are allowable.

Accordingly, the rejections to these claims should be withdrawn.

e. Claim 14

As provided in independent claim 14, Applicant claims:

> A system for rerouting the transmission of data to avoid a firewall, the system comprising: a transmission device configured to ***search for a firewall protecting a destination at a remote network***, the firewall at the remote network being configured to prohibit communication to the destination via a primary communication protocol and allow communication to the destination via a secondary communication protocol, the transmission device is further configured to, ***upon detection of the firewall, automatically configure the data for communication over the secondary communication protocol and transmit the data by utilizing the secondary communication protocol, wherein the transmission device is further configured to receive a request to transmit the data to the destination and the request comprises at least the following: a primary address and a secondary address of the destination, the primary address being related to the primary communication protocol and the secondary address being related to the secondary communication protocol and wherein the transmission device is further configured to, upon not detecting the firewall, transmit the data to the destination by utilizing the primary communication protocol***.

(Emphasis added).

Applicant respectfully submits that independent claim 14 is allowable for at least the reason that *Schwartz* does not disclose, teach, or suggest at least a transmission device configured to "search for a firewall protecting a destination at a remote network," "upon detection of the firewall, automatically configure the data for communication over the secondary communication

protocol and transmit the data by utilizing the secondary communication protocol," and "wherein the transmission device is further configured to receive a request to transmit the data to the destination and the request comprises at least the following: a primary address and a secondary address of the destination, the primary address being related to the primary communication protocol and the secondary address being related to the secondary communication protocol and wherein the transmission device is further configured to, upon not detecting the firewall, transmit the data to the destination by utilizing the primary communication protocol," as recited and emphasized above.

Rather, *Schwartz* discloses at most a system for configuring a device to communicate through a firewall on a local network, where the device is also located on the local network. *See* paras. 0024-0025 and Figure 3 (*e.g.*, devices 312, 314, and firewall 310). *Schwartz* fails to teach or suggest searching for a firewall protecting a destination at a remote network.

*Schwartz* also states that "if an address and/or port does not yield a successful connection, then the next time the device will select the most likely address and port 506, it may not include the unsuccessful port." *See* para. 0032. "It is to be understood that select most likely address and port 506 is based upon a database of addresses and ports and that this database changes." *See* para. 0032. Therefore, *Schwartz* fails to teach or suggest that a request to transmit data includes a primary address of the destination that is used if a firewall is not detected and a secondary address of the destination that is used if a firewall is detected, as described in the claim. Rather, *Schwartz* uses whatever port the non-traditional device discerns is most likely to establish a connection with the local firewall. As such, *Schwartz* fails to teach or suggest that a request to transmit data includes a primary address and a secondary address of a firewall associated with a destination. As previously indicated, *Schwartz* teaches that a local device is configured to operate with a local firewall by attempting different addresses for the local firewall. Accordingly, no where does it teach or suggest attempting to communicate with a firewall associated with a destination at a remote network in a manner described by the claim.

For at least these reasons, *Schwartz* fails to anticipate claim 14. In the Office Action, it states that "the client shown in Fig. 3 may have to pass the firewall associated with the appliances in the remote network to control them." Page 3. However, no where in *Schwartz* does it state that the clients 308-1...308-N shown in Fig. 3 perform the method for firewall traversal disclosed in the reference. Rather, the non-traditional devices 314-1...314-Q are disclosed to employ the method for firewall traversal described in the reference which states "This information must be transferred from the non-traditional device across the LAN 311 through the firewall 310 to a destination." Para. 0025. Another example is provided in *Schwartz* of a home entertainments system 314-5 that must traverse the local firewall 310 to access the manufacturer's site. As such, *Schwartz* does not teach to "search for a firewall protecting a destination at a remote network . . . wherein the transmission device is further configured to receive a request to transmit the data to the destination and the request comprises at least the following: a primary address and a secondary address of the destination, the primary address being related to the primary communication protocol and the secondary address being related to the secondary communication protocol and wherein the transmission device is further configured to, upon not detecting the firewall, transmit the data to the destination by utilizing the primary communication protocol," as recited in claim 14.

Moreover, the Office Action states that "It is true that Scharwtz won't try the primary address again if it fails, but it clearly tries it the first time, which was before the connection failed. Therefore, the address of the primary and secondary protocols must be received by the device that initiates the connection." Page 4. Applicants respectfully disagree, since *Schwartz* teaches that an address may be obtained by sniffing network traffic and therefore does not have to be "received by the device that initiates the connection." Further, *Schwartz* does not teach or suggest that a request to transmit data comprises both the primary address and secondary address of the destination, as described in claim 14.

For at least these reasons, *Schwartz* fails to anticipate claim 14, and the rejection of claim 14 should be withdrawn.

f. Claims 17-28

Because independent claim 14 is allowable over the cited art of record, dependent claims 17-28 (which depend from independent claim 14) are allowable as a matter of law for at least the reason that the dependent claims 17-28 contain all the elements and features of independent claim 14. For at least this reason, the rejection of claims 17-28 should be withdrawn.

Additionally and notwithstanding the foregoing reasons for allowability of claims 17-28, these claims recite further features and/or combinations of features (as is apparent by examination of the claims themselves) that are patentably distinct from the cited art of record. Hence, there are other reasons why these dependent claims are allowable.

Accordingly, the rejections to these claims should be withdrawn.

g. Claim 29

As provided in independent claim 29, Applicant claims:

> A transmission device configured to transmit data to a destination, the transmission device comprising:
> means for transmitting the data to the destination at a remote network by utilizing a secondary communication protocol;
> ***means for searching for a firewall at the remote network, the firewall being configured to prohibit communication to the destination by a primary communication protocol and allow communication to the destination via the secondary communication protocol;***
> ***means for automatically configuring the data for communication for the secondary communication protocol upon detecting the firewall; and***
> ***means for receiving a request to transmit the data to the destination, wherein the request comprises at least the following:***
> ***a primary address and a secondary address of the destination, the primary address being related to the primary communication protocol and the secondary address being related to the secondary communication protocol.***

(Emphasis added).

Applicant respectfully submits that independent claim 29 is allowable for at least the reason that *Schwartz* does not disclose, teach, or suggest at

least "means for searching for a firewall at the remote network, the firewall being configured to prohibit communication to the destination by a primary communication protocol and allow communication to the destination via the secondary communication protocol," "means for automatically configuring the data for communication for the secondary communication protocol upon detecting the firewall," and "means for receiving a request to transmit the data to the destination, wherein the request comprises at least the following: a primary address and a secondary address of the destination, the primary address being related to the primary communication protocol and the secondary address being related to the secondary communication protocol," as recited and emphasized above.

Rather, *Schwartz* discloses at most a system for configuring a device to communicate through a firewall on a local network, where the device is also located on the local network. *See* paras. 0024-0025 and Figure 3 (*e.g.*, devices 312, 314, and firewall 310). *Schwartz* fails to teach or suggest searching for a firewall at a remote network in the manner described in the claim.

*Schwartz* also states that "if an address and/or port does not yield a successful connection, then the next time the device will select the most likely address and port 506, it may not include the unsuccessful port." *See* para. 0032. "It is to be understood that select most likely address and port 506 is based upon a database of addresses and ports and that this database changes." *See* para. 0032. Therefore, *Schwartz* fails to teach or suggest that a request to transmit data includes a primary address of the destination that is used if a firewall is not detected and a secondary address of the destination that is used if a firewall is detected, as described in the claim. Rather, *Schwartz* uses whatever port the non-traditional device discerns is most likely to establish a connection with the local firewall. As such, *Schwartz* fails to teach or suggest that a request to transmit data includes a primary address and a secondary address of a firewall associated with a destination. As previously indicated, *Schwartz* teaches that a local device is configured to operate with a local firewall by attempting different addresses for the local firewall. Accordingly, no where does it teach or suggest attempting to

communicate with a firewall associated with a destination at a remote network in a manner described by the claim.

For at least these reasons, *Schwartz* fails to anticipate claim 29. In the Office Action, it states that "the client shown in Fig. 3 may have to pass the firewall associated with the appliances in the remote network to control them." Page 3. However, no where in *Schwartz* does it state that the clients 308-1...308-N shown in Fig. 3 perform the method for firewall traversal disclosed in the reference. Rather, the non-traditional devices 314-1...314-Q are disclosed to employ the method for firewall traversal described in the reference which states "This information must be transferred from the non-traditional device across the LAN 311 through the firewall 310 to a destination." Para. 0025. Another example is provided in *Schwartz* of a home entertainments system 314-5 that must traverse the local firewall 310 to access the manufacturer's site. As such, *Schwartz* does not teach "means for searching for a firewall at the remote network, the firewall being configured to prohibit communication to the destination by a primary communication protocol and allow communication to the destination via the secondary communication protocol . . . wherein the request comprises at least the following: a primary address and a secondary address of the destination, the primary address being related to the primary communication protocol and the secondary address being related to the secondary communication protocol," as recited in claim 29.

Moreover, the Office Action states that "It is true that Scharwtz won't try the primary address again if it fails, but it clearly tries it the first time, which was before the connection failed. Therefore, the address of the primary and secondary protocols must be received by the device that initiates the connection." Page 4. Applicants respectfully disagree, since *Schwartz* teaches that an address may be obtained by sniffing network traffic and therefore does not have to be "received by the device that initiates the connection." Further, *Schwartz* does not teach or suggest that a request to transmit data comprises both the primary address and secondary address of the destination, as described in claim 29.

For at least these reasons, *Schwartz* fails to anticipate claim 29, and the rejection of claim 29 should be withdrawn.

h. Claims 30 and 33-34

Because independent claim 29 is allowable over the cited art of record, dependent claims 30 and 33-34 (which depend from independent claim 29) are allowable as a matter of law for at least the reason that the dependent claims 30 and 33-34 contain all the elements and features of independent claim 29. For at least this reason, the rejection of claims 30 and 33-34 should be withdrawn.

Additionally and notwithstanding the foregoing reasons for allowability of claims 30 and 33-34, these claims recite further features and/or combinations of features (as is apparent by examination of the claims themselves) that are patentably distinct from the cited art of record. Hence, there are other reasons why these dependent claims are allowable.

Accordingly, the rejections to these claims should be withdrawn.

i. Claim 35

As provided in independent claim 35, Applicant claims:

> A data transmission program stored on a computer-readable medium, the transmission program comprising:
> logic configured to facilitate the transmission of data to a remote network by utilizing a secondary communication protocol;
> ***logic configured to search for a firewall at the remote network, wherein the firewall is configured to prohibit communication to a recipient device at the remote network via a primary communication protocol and allow communication via the secondary communication protocol;*** and
> ***logic configured to automatically configure communication for the secondary communication protocol upon detecting the firewall;*** and
> ***logic configured to receive a request to transmit the data to the recipient device, the request comprising of at least the following: a primary address and a secondary address of the recipient device, the primary address being related to the primary communication protocol and the***

***secondary address being related to the secondary communication protocol.***

(Emphasis added).

Applicant respectfully submits that independent claim 35 is allowable for at least the reason that *Schwartz* does not disclose, teach, or suggest at least "logic configured to search for a firewall at a remote network, wherein the firewall is configured to prohibit communication to a recipient device at the remote network via a primary communication protocol and allow communication via the secondary communication protocol," "logic configured to automatically configure communication for the secondary communication protocol upon detecting the firewall," and "logic configured to receive a request to transmit the data to the recipient device, the request comprising of at least the following: a primary address and a secondary address of the recipient device, the primary address being related to the primary communication protocol and the secondary address being related to the secondary communication protocol," as recited and emphasized above.

Rather, *Schwartz* discloses at most a system for configuring a device to communicate through a firewall on a local network, where the device is also located on the local network. *See* paras. 0024-0025 and Figure 3 (*e.g.*, devices 312, 314, and firewall 310). *Schwartz* fails to teach or suggest searching for a firewall at a remote network in the manner described in the claim.

*Schwartz* also states that "if an address and/or port does not yield a successful connection, then the next time the device will select the most likely address and port 506, it may not include the unsuccessful port." *See* para. 0032. "It is to be understood that select most likely address and port 506 is based upon a database of addresses and ports and that this database changes." *See* para. 0032. Therefore, *Schwartz* fails to teach or suggest that a request to transmit data includes a primary address of the destination that is used if a firewall is not detected and a secondary address of the destination that is used if a firewall is detected, as described in the claim. Rather, *Schwartz* uses whatever port the non-traditional device discerns is most likely to establish a connection with the local firewall. As such, *Schwartz* fails to

teach or suggest that a request to transmit data includes a primary address and a secondary address of a firewall associated with a destination. As previously indicated, *Schwartz* teaches that a local device is configured to operate with a local firewall by attempting different addresses for the local firewall. Accordingly, no where does it teach or suggest attempting to communicate with a firewall associated with a destination at a remote network in a manner described by the claim.

For at least these reasons, *Schwartz* fails to anticipate claim 35. In the Office Action, it states that "the client shown in Fig. 3 may have to pass the firewall associated with the appliances in the remote network to control them." Page 3. However, no where in *Schwartz* does it state that the clients 308-1...308-N shown in Fig. 3 perform the method for firewall traversal disclosed in the reference. Rather, the non-traditional devices 314-1...314-Q are disclosed to employ the method for firewall traversal described in the reference which states "This information must be transferred from the non-traditional device across the LAN 311 through the firewall 310 to a destination." Para. 0025. Another example is provided in *Schwartz* of a home entertainments system 314-5 that must traverse the local firewall 310 to access the manufacturer's site. As such, *Schwartz* does not teach "logic configured to search for a firewall at a remote network . . . and logic configured to receive a request to transmit the data to the recipient device, the request comprising of at least the following: a primary address and a secondary address of the recipient device, the primary address being related to the primary communication protocol and the secondary address being related to the secondary communication protocol," as recited in claim 35.

Moreover, the Office Action states that "It is true that Scharwtz won't try the primary address again if it fails, but it clearly tries it the first time, which was before the connection failed. Therefore, the address of the primary and secondary protocols must be received by the device that initiates the connection." Page 4. Applicants respectfully disagree, since *Schwartz* teaches that an address may be obtained by sniffing network traffic and therefore does not have to be "received by the device that initiates the connection." Further, *Schwartz* does not teach or suggest that a request to

transmit data comprises both the primary address and secondary address of the destination, as described in claim 35.

For at least these reasons, *Schwartz* fails to anticipate claim 35, and the rejection of claim 35 should be withdrawn.

j. Claims 37 and 39-41

Because independent claim 35 is allowable over the cited art of record, dependent claims 37 and 39-41 (which depend from independent claim 35) are allowable as a matter of law for at least the reason that the dependent claims 37 and 39-41 contain all the features of independent claim 35. For at least this reason, the rejection of claims 37 and 39-41 should be withdrawn.

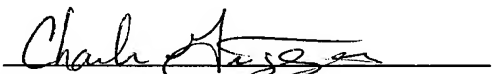
Additionally and notwithstanding the foregoing reasons for allowability of claims 37 and 39-41, these claims recite further features and/or combinations of features (as is apparent by examination of the claims themselves) that are patentably distinct from the cited art of record. Hence, there are other reasons why these dependent claims are allowable.

Accordingly, the rejections to these claims should be withdrawn.

## *CONCLUSION*

For at least the reasons set forth above, Applicant respectfully submits that all objections and/or rejections have been traversed, rendered moot, and/or accommodated, and that the pending claims are in condition for allowance. Favorable reconsideration and allowance of the present application and all pending claims are hereby courteously requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned agent at (770) 933-9500.

Respectfully submitted,



**Charles W. Griggers**
**Reg. No. 47,283**